

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (previously presented) A method of preventing an attack on a network, the method comprising the computer-implemented steps of:
  - receiving a request to access a resource from a user, wherein the request includes an accumulated work value;
  - wherein the accumulated work value represents a total amount of work previously performed by the user and accumulated across multiple prior requests by the user;
  - receiving a prior keyless user identity value  $H(i+1, x)$  in the request comprising a one-time password, wherein  $H(i+1, x)$  is computed by the user as a hash chain from a non-shared user secret ( $x$ ), wherein  $H(n, x) = h(H(n-1, x))$ , wherein  $n > 0$  and  $H(0, x) = x$ , wherein function  $h$  is a one-way function that is difficult to invert;
  - receiving a current user identity value  $H(i, x)$ ;
  - verifying that the keyless user identity value properly identifies the user only upon determining that  $h(H(i, x)) = H(i+1, x)$ ;
  - wherein  $h$  comprises a SHA-1 hash algorithm;
  - wherein  $n$  is between  $10^4$  and  $10^6$ ;
  - determining whether the accumulated work value exceeds a required work threshold value, and if not, requiring the user to perform a quantity of work as a condition for accessing the resource;
  - providing the user with access to the resource;
  - determining an amount of accumulated work output value to provide to the user based on a volume of data communicated between the resource and the user; and
  - wherein the accumulated work output value represents a second amount of work performed by the user;
  - providing the accumulated work output value to the user.

2. (original) A method as recited in Claim 1, wherein the request includes a prior user identity value and a current user identity value, and further comprising the steps of determining whether a mathematical relationship of the current user identity value and the prior user identity value indicates that the user has possession of a resource secret.

3.-5. (cancelled)

6. (original) A method as recited in Claim 1, further comprising the step of determining the required work threshold value based on a then-current capacity of the resource.

7. (currently amended) A method as recited in Claim 1, further comprising the steps of:  
determining the required work threshold value based on a then-current capacity of the resource;  
requiring a first user who has ~~an~~ a first accumulated work value that is greater than the required work threshold value to perform a first amount of work as a condition for accessing the resource; and  
requiring a second user who has ~~an~~ a second accumulated work value that is less than or equal to the required work threshold value to perform a second amount of work as a condition for accessing the resource, wherein the second amount of work is greater than the first amount of work.

8. (currently amended) A method as recited in Claim 1, wherein the step of determining ~~an~~ the amount of accumulated work output value is performed for a specified user only during a specified time period in which accumulating work is allowed for that specified user.

9. (currently amended) A method as recited in Claim 1, wherein the step of determining ~~an~~ the amount of accumulated work output value is performed for a specified user only if the current user identity value received from the user is not found in a list of user identity values that were previously received in a specified time period.

10. (currently amended) A method as recited in Claim 1, further comprising the step of digitally signing and providing a timestamp to the user with the accumulated work output value, and wherein the step of determining ~~an~~ the amount of accumulated work output value is performed for a specified user only upon:

receiving the timestamp is received in a subsequent request;  
verifying the timestamp value; and  
determining that the timestamp value is within an allowed range.

11. (currently amended) A method as recited in Claim 1, further comprising the step of receiving the accumulated ~~proof of~~ work value, a prior user identity value and a current user identity value in a cookie provided by the user to the resource.

12. (currently amended) A method as recited in Claim 1, wherein determining ~~an~~ the amount of accumulated work output value to provide to the user based on a the volume of data communicated between the resource and the user comprises determining the amount of accumulated work output value as  $2^k * p$ , where k is a number of bits of work previously performed by the user and p is a number of messages or packets communicated between the user and the resource.

13. (original) A method as recited in Claim 1, further comprising the step of providing the accumulated work output value in a cookie sent from the resource to the user.

14. (original) A method as recited in Claim 1, further comprising the step of selectively increasing the required work threshold value for a particular user in response to congestion conditions of the resource.

15. (currently amended) A method as recited in Claim 1, wherein requiring the user to perform a the quantity of work as a condition for accessing the resource comprises requiring the user to hash a message until a specified number of bits are zero.

16. (currently amended) A method of preventing an attack on a network, the method comprising computer-implemented steps of:
- receiving a request to access a resource from a user, wherein the request includes an accumulated work value that represents work that the resource has previously required the user to perform in order to obtain previous access to the resource;
  - receiving a prior keyless user identity value  $H(i+1,x)$  in the request comprising a one-time password, wherein  $H(i+1,x)$  is computed by the user as a hash chain from a non-shared user secret ( $x$ ), wherein  $H(n,x) = h(H(n-1,x))$ , wherein  $n > 0$  and  $H(0,x) = x$ , wherein function  $h$  is a one-way function that is difficult to invert;
  - receiving a current user identity value  $H(i,x)$ ;
  - verifying that the keyless user identity value properly identifies the user only upon determining that  $h(H(i,x)) = H(i+1,x)$ ;
  - wherein  $h$  comprises a SHA-1 hash algorithm;
  - wherein  $n$  is between  $10^4$  and  $10^6$ ;
  - determining whether the accumulated work value exceeds a required work threshold value; and
  - providing the user with access to the resource only when the accumulated work value exceeds ~~a~~ the required work threshold value.
17. (previously presented) An apparatus, comprising
- one or more processors;
  - means for receiving a request to access a resource from a user, wherein the request includes an accumulated work value;
  - wherein the accumulated work value represents a total amount of work previously performed by the user and accumulated across multiple prior requests by the user;
  - means for receiving a prior keyless user identity value  $H(i+1,x)$  in the request comprising a one-time password, wherein  $H(i+1,x)$  is computed by the user as a hash chain from a non-shared user secret ( $x$ ), wherein  $H(n,x) = h(H(n-1,x))$ , wherein  $n > 0$  and  $H(0,x) = x$ , wherein function  $h$  is a one-way function that is difficult to invert;
  - means for receiving a current user identity value  $H(i,x)$ ;

means for verifying that the keyless user identity value properly identifies the user only  
upon determining that  $h(H(i,x)) = H(i+1,x)$ ;

wherein  $h$  comprises a SHA-1 hash algorithm;

wherein  $n$  is between  $10^4$  and  $10^6$ ;

means for determining whether the accumulated work value exceeds a required work  
threshold value, and if not, requiring the user to perform a quantity of work as a  
condition for accessing the resource;

means for providing the user with access to the resource;

means for determining an amount of accumulated work output value to provide to the  
user based on a volume of data communicated between the resource and the user;  
and

wherein the accumulated work output value represents a second amount of work  
performed by the user;

means for providing the accumulated work output value to the user.

18. (previously presented) An apparatus, comprising:

a processor;

a computer-readable volatile or non-volatile medium storing one or more stored  
sequences of instructions that are accessible to the processor, wherein execution  
of the one or more stored sequences of instructions by the processor causes the  
processor to perform:

receiving a request to access a resource from a user, wherein the request includes an  
accumulated work value;

wherein the accumulated work value represents a total amount of work previously  
performed by the user and accumulated across multiple prior requests by the user;

receiving a prior keyless user identity value  $H(i+1,x)$  in the request comprising a one-time  
password, wherein  $H(i+1,x)$  is computed by the user as a hash chain from a non-  
shared user secret ( $x$ ), wherein  $H(n,x) = h(H(n-1,x))$ , wherein  $n > 0$  and  $H(0,x) = x$ ,  
wherein function  $h$  is a one-way function that is difficult to invert;

receiving a current user identity value  $H(i,x)$ ;

- verifying that the keyless user identity value properly identifies the user only upon  
determining that  $h(H(i,x)) = H(i+1,x)$ ;  
wherein  $h$  comprises a SHA-1 hash algorithm;  
wherein  $n$  is between  $10^4$  and  $10^6$ ;  
determining whether the accumulated work value exceeds a required work threshold  
value, and if not, requiring the user to perform a quantity of work as a condition  
for accessing the resource;  
providing the user with access to the resource;  
determining an amount of accumulated work output value to provide to the user based on  
a volume of data communicated between the resource and the user; and  
wherein the accumulated work output value represents a second amount of work  
performed by the user;  
providing the accumulated work output value to the user.
19. (previously presented) A computer-readable volatile or non-volatile medium storing one or more sequences of instructions, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform:  
receiving a request to access a resource from a user, wherein the request includes an accumulated work value;  
wherein the accumulated work value represents a total amount of work previously performed by the user and accumulated across multiple prior requests by the user;  
receiving a prior keyless user identity value  $H(i+1,x)$  in the request comprising a one-time password, wherein  $H(i+1,x)$  is computed by the user as a hash chain from a non-shared user secret ( $x$ ), wherein  $H(n,x) = h(H(n-1,x))$ , wherein  $n > 0$  and  $H(0,x) = x$ , wherein function  $h$  is a one-way function that is difficult to invert;  
receiving a current user identity value  $H(i,x)$ ;  
verifying that the keyless user identity value properly identifies the user only upon  
determining that  $h(H(i,x)) = H(i+1,x)$ ;  
wherein  $h$  comprises a SHA-1 hash algorithm;  
wherein  $n$  is between  $10^4$  and  $10^6$ ;

- determining whether the accumulated work value exceeds a required work threshold value, and if not, requiring the user to perform a quantity of work as a condition for accessing the resource;
- providing the user with access to the resource;
- determining an amount of accumulated work output value to provide to the user based on a volume of data communicated between the resource and the user; and
- wherein the accumulated work output value represents a second amount of work performed by the user;
- providing the accumulated work output value to the user.
20. (previously presented) The computer-readable storage medium of Claim 19, wherein the request includes a prior user identity value and a current user identity value, and further comprising instructions which when executed by the one or more processors cause determining whether a mathematical relationship of the current user identity value and the prior user identity value indicates that the user has possession of a resource secret.
21. (currently amended) The computer-readable storage medium of Claim 19, further comprising instructions which when executed by the one or more processors cause:
- determining the required work threshold value based on a then-current capacity of the resource;
- requiring a first user who has ~~an~~ a first accumulated work value that is greater than the required work threshold value to perform a first amount of work as a condition for accessing the resource; and
- requiring a second user who has ~~an~~ a second accumulated work value that is less than or equal to the required work threshold value to perform a second amount of work as a condition for accessing the resource, wherein the second amount of work is greater than the first amount of work.
22. (currently amended) The computer-readable storage medium of Claim 19, wherein the instructions for determining ~~an~~ the amount of accumulated work output value are performed for a

specified user only if the current user identity value received from the user is not found in a list of user identity values that were previously received in a specified time period.

23. (currently amended) The computer-readable storage medium of Claim 19, further comprising instructions previously presented when executed by the one or more processors cause digitally signing and providing a timestamp to the user with the accumulated work output value, and wherein the instructions for determining ~~an~~ the amount of accumulated work output value are performed for a specified user only upon:

receiving the timestamp is received in a subsequent request;  
verifying the timestamp value; and  
determining that the timestamp value is within an allowed range.

24. (previously presented) The apparatus of Claim 17, wherein the request includes a prior user identity value and a current user identity value, and further comprising means for determining whether a mathematical relationship of the current user identity value and the prior user identity value indicates that the user has possession of a resource secret.

25. (currently amended) The apparatus of Claim 17, further comprising:  
means for determining the required work threshold value based on a then-current capacity of the resource;  
means for requiring a first user who has ~~an~~ a first accumulated work value that is greater than the required work threshold value to perform a first amount of work as a condition for accessing the resource; and  
means for requiring a second user who has ~~an~~ a second accumulated work value that is less than or equal to the required work threshold value to perform a second amount of work as a condition for accessing the resource, wherein the second amount of work is greater than the first amount of work.

26. (currently amended) The apparatus of Claim 17, wherein means for determining ~~an~~ the amount of accumulated work output value is operable for a specified user only if the current user



identity value received from the user is not found in a list of user identity values that were previously received in a specified time period.

27. (currently amended) The apparatus of Claim 17, further comprising means for digitally signing and providing a timestamp to the user with the accumulated work output value, and wherein the means for determining ~~an~~ the amount of accumulated work output value is operable for a specified user only upon:

receiving the timestamp is received in a subsequent request;  
verifying the timestamp value; and  
determining that the timestamp value is within an allowed range.

28. (previously presented) The apparatus of Claim 18, wherein the request includes a prior user identity value and a current user identity value, and further comprising instructions which when executed by the processor cause determining whether a mathematical relationship of the current user identity value and the prior user identity value indicates that the user has possession of a resource secret.

29. (currently amended) The apparatus of Claim 18, further comprising instructions which when executed by the processor cause:

determining the required work threshold value based on a then-current capacity of the resource;

requiring a first user who has ~~an~~ a first accumulated work value that is greater than the required work threshold value to perform a first amount of work as a condition for accessing the resource; and

requiring a second user who has ~~an~~ a second accumulated work value that is less than or equal to the required work threshold value to perform a second amount of work as a condition for accessing the resource, wherein the second amount of work is greater than the first amount of work.

30. (currently amended) The apparatus of Claim 18, wherein the instructions for determining ~~an~~ the amount of accumulated work output value are performed for a specified user only if the

current user identity value received from the user is not found in a list of user identity values that were previously received in a specified time period.

31. (currently amended) The apparatus of Claim 18, further comprising instructions which when executed by the processor cause digitally signing and providing a timestamp to the user with the accumulated work output value, and wherein instructions for determining ~~an~~ the amount of accumulated work output value is performed for a specified user only upon:

- receiving the timestamp is received in a subsequent request;
- verifying the timestamp value; and
- determining that the timestamp value is within an allowed range.